1416.01 Electronic Asset Management Standard
Issued May 1, 2000

SUBJECT: Electronic Asset Management Standard

APPLICATION: All Executive agencies and other non-executive branch entities.

PURPOSE: Present the features and functionality required by the State of Michigan for an enterprise-wide Electronic Asset Management solution.

CONTACT AGENCY: Department of Information Technology (DIT)
Bureau of Strategic Policy

TELEPHONE: 517/373-7326

FAX: 517/335-2355

SUMMARY: Consulting services may be required when an agency is moving, adding, or changing telecommunication services.

APPLICABLE FORMS: None.
CONTENTS:

- 5.2 Target Network Support
- 5.3 Available Platforms for Domain Distribution Servers

1.0 INTRODUCTION

The State has invested significant resources into desktop, mobile, and network computing devices in order to build a computing infrastructure for performing a wide variety of tasks required to properly execute the State's mission.

Managing these computing resources effectively has become essential due to the sheer number of microcomputers, growing client / server technology usage, more powerful desktop applications and operating systems, increasing importance of server applications, reduced support budgets, reduced staff, and expanded remote connectivity.

In November of 1995, an Electronic Asset Management committee formed with State agency representatives. Over the course of six months, the group developed and finalized a list of requirements representing the State's needed EAM functionality.

Electronic Asset Management (EAM) covers the areas of electronic software distribution, hardware and software inventory, software license management, remote troubleshooting, and virus protection.

Benefits of EAM include improvements in upgrade and purchase planning, user productivity, software license compliance, capital asset tracking, and configuration management. EAM can result in reduced software distribution costs that are predictable, plus faster deployment. Software purchased can be more accurately matched to actual needs due to usage reporting.

This Electronic Asset Management Standard represents the functionality required by the State of Michigan to implement a strategic enterprise-wide Electronic Asset Management System. The technology to implement this Standard in a cost-effective manner does not yet exist. Guideline 1416.02 has been developed to present a short term tactical solution to address the State's Electronic Asset Management needs, until such time as technology can support a strategic enterprise-wide solution in our environment.

2.0 ELECTRONIC SOFTWARE DISTRIBUTION (ESD)

2.1 VERSION CONTROL:

Product must provide active version checking upon user software activation/request.

Product should allow configurations where the user can elect to proceed with and outdated client.

The product must allow configurations where the client is blocked form loading out of date client software and must accept a version update prior to proceeding.

The product should allow configurations where the client is blocked from loading out of date client software and is informed that the update will occur at a scheduled time in an unattended mode.

Product must allow multiple versions of the same software product on the same client.

2.2 DISTRIBUTION MANAGEMENT

Product must support both push and pull ESD strategies.

Product must allow electronic software distribution at user log-on.

The ESD system must also provide flexible scheduling routines, which allow software distribution to be scheduled and distributed at a time other than user log-on.

The ESD system must provide the ability to support unattended operations, so that user does not have to be present to distribute software.

The ESD system must be able to immediately distribute software or files on demand by specifically authorized personnel. (i.e. software distributed by help desk)

Product must support roll back to a previous version of the software or file if desired.

Must allow the user of package definition files, scripting language, or similar functionality to control distribution on target workstations.

The ESD system must support data compression to reduce network traffic.

For both push and pull configurations, the user must be able to accept, reject, or reschedule software distributions.

The ESD must verify essential client resources such as available disk space before commencing the distribution/installation.

Product must verify that all prerequisite hardware and software components exist before a distribution takes place.

The status of Statewide distributions should be able to be monitored.

2.3 DISTRIBUTION AGENTS:

The distribution agent whjch resides on the workstation must consume a minimum amount of system memory (such as a virtual driver) and not conflict with other software, or extensions under Macs.

Ability to distribute new versions of the agent automatically.

The distribution agent must be able to check that there is available disk space and other critical client resources before initiating a distribution.

Distribution agents should be easy to install and be able to be installed through the ESD software.

Initial agent installation should be automatic without client effort at the point of log-in to the network.

Agent upgrades should be backward compatible.

The agent should cleanup in the event of a failed distribution.

The agent residing on the client workstation should not impede the operations of other applications from running effectively and efficiently.

The agent should integrate with other system management or network management tools used by State agencies.

2.4 DIAL-UP WORKSTATIONS:

The ESD system must be able to distribute software to dial-up workstations. Upcoming upgrade notifications to users should be distributable by state's e-mail environment.

Users must have the ability to refuse an upgrade when using slow transmission facilities.

2.5 DISTRIBUTION:

Must be able to distribute all kinds of software and files, including, but not limited to:
single files, such as dynamic link libraries to the workstation/server
virus checking software to workstations/servers
virus checking database updates to the workstation/server
desktop software applications to the workstation
new versions of platform operating systems to the workstation/server
e-mail software to the workstation
new versions of terminal emulation software
network stacks (TCP/IP, IPX, Vines IP) to workstations/servers
Workstation/server security software

Be capable of delivering only changed files within a package of files.

Be capable of delivering only the changes to be made to target files.

Macintosh distributions must also place all control and extensions in proper folders.

Distribution outcome reporting should be available to both top-most distribution point, as well as any lower domain level.

2.6 DISTRIBUTION STAGING SERVERS:

Product must support multiple tiers of Staging servers (i.e. Statewide server, agency-wide staging server, physical location staging server, etc.)

Staging servers should have adequate security.

The staging servers must support centralized and decentralized (agency) administration.

Can be configured to control distributions from superordinate servers.

Can be used to distribute items unique to the domain controlled by the distribution server.

Can allow a distribution originating in a given domain to be distributed to another parallel domain.

Product should be able to pass installation packages to distributors contained in such LAN administrative packages as LANDesk Manager and SMS.

Such package transfer capability should be accompanied with the ability return distribution confirmation notice from the LAN administrator to this vendor product.

2.7.1 WINDOWS AND DOS SOFTWARE INSTALLATION

Product should be able to distribute and update windows software applications.

Product should be able to distribute new versions of Windows, including Windows/95 and Windows/NT.

Product should provide the ability to update application configuration files.

Product should provide the ability to update application configuration files.

Provide ability to update or replace Dynamic Link Libraries (DLLs).

Provide ability to update Autoexec.bat and Config.sys files.

Provide ability to update win.ini and system.ini files.

Provide ability to update registration database.

Provide ability to support various monitor configurations supported by Windows.

Provide ability to support various printer configurations supported by Windows.

The ESD should be able to update program manager groups and items.

Product can modify properties of existing icons.

Product can add icons in windows and groups.

Product can precede installations with bat files that can modify INI and Config files.

Product must be able to conduct NT workstation software installations by accommodating NT security, use of a PDL file, modifying the register, and performing a remote boot.

2.7.2 NETWORK SOFTWARE INSTALLATION

The ESD should be able to install network software components such as TCP/IP stacks and update Net.config files for NetWare.

The ESD must have protection mechanism to prevent overwriting TCP/IP configuration information and addresses.

Product can structure packages that allow protocol stacks and drivers to be installed prior to the applications.

2.7.3 MACINTOSH SOFTWARE INSTALLATION

Product should be able to install Macintosh software applications with the appropriate installer application.

Product should be able to distribute new versions of Macintosh O/S including Copeland.

2.7.4 MISCELLANEOUS INSTALLATION ITEMS

Product can address the scripting demands and command line processes in OS/2.

Product should be able to perform a deinstallation, including removal of icons and related GUI items.

2.8 ESD AUDIT TRAIL

Flexible report writing capabilities should be provided with the system.

A complete audit trail or what was distributed to each workstation should be maintained and be available for queries and reports.

The ESD system must provide reporting on failed or rejected distributions at all levels.

Audit reporting should incorporate ad hoc techniques.

2.9 CONFIGURATION MANAGEMENT

Product must support defined standard configurations. Product must have the capability to configure client workstations based on standard configurations.

Product should support multiple configurations to support different versions and releases of software.

Configurations should be easy to maintain using GUI and object management techniques.

Changes to standard configurations should be able to be distributed via domain staging (distribution) servers.

Product must support an active monitoring of all client and server configurations for identification of instances of changes from standard configurations.

2.10 USABILITY AND SECURITY

Maintenance functions should be straightforward and easy to use. That is, adding new items to the inventory should be able to use models or scripts, and they should be readily available from the vendor.

Creating installation scripts should be easy and straightforward.

Product should have well designed and established security routines.

Product should have virus detection and prevention to prevent viruses from being disseminated throughout the network.

Integration with existing network infrastructure should be easy and straightforward.

Product must allow distribution package originator to invoke resident virus package to screen prepared files/package prior to distribution.

Product should allow distribution server point to invoke domain resident virus package to screen incoming package for distribution within that domain.

Product should allow the client the option to preclude remote distribution/installation.

3.0 ELECTRONIC INVENTORY AND LICENSE MANAGEMENT:
3.1 LICENSE MANAGEMENT

Product must have the ability to track license information of installed software.

The system must have the capability to track the date and price paid for software licenses, PO number, source, agency, etc.

Product must be able to generate warnings when license counts are exceeded.

When software is removed from a client or server, the product should allow the automatic inclusion of that license in an "available" pool of licenses for transfer to other devices.

3.2 SOFTWARE METERING

Product should have a metering component to measure use of licensed software.

Based on the option of the system administrator, the system should be able to restrict usage or send a notification after a threshold has been exceeded.

Product must maintain statistics on average and peak usage.

It should support software suites as well as individual products.

Product should have ad hoc reporting capabilities.

Product should allow users drawing on license availability across domains.

3.3 INVENTORY DATABASE

Product must use a SQL-compliant relational database to maintain inventory and configuration information. If the product is not SQL compliant, then the product must support data exports to a SQL database. Export routines must be provided for various databases including Oracle, and SQL Server.

The database must be able to be modified or extended by systems staff.

Removing items from inventory should be easy and straightforward.

An inventory history must be maintained for each client and server.

Product should support a "side by side" comparison of current condition to the previous condition.

Inventory information should be able to be maintained by site or network segment.

Inventory information should be able to be maintained on dial-up workstations.

Inventory information should be easily accessible by help desk personnel.

Additional information such as user's name should be able to be added to the inventory data.

The database architecture must support an enterprise-wide data repository (this aspect must be described in detail).

Product must include a sound database disaster recovery provision (this aspect must be described in detail).

Product must capture the version numbers of software it discovers. If a version number does not exists, then it should capture the size and date of the primary executable file.

3.4 INVENTORY MANAGEMENT

Product must have built-in inventory system.

Product must have auto discovery capabilities, scheduled discovery by date, or scheduled discovery by network segment.

Product must be able to inventory software loaded on clients, servers, and other common-serving devices.

Product should be able to capture version and release information on software.

Product should be able to capture hardware configuration information including RAM, hard disk size, etc.

Product should be able to capture CMOS information.

Product should be able to capture information about device drivers.

Collection of inventory information should be able to be scheduled and performed in off hours.

Product should be able to report deltas or changes to inventories.

Product should be able to capture TCP/IP address information.

Product should have an extensive software discovery dictionary to identify the wide array of software packages used by the State.

Product must be able to discover the installation of custom software packages written by the State.

Product should allow items to be entered manually into the inventory database

3.5 INVENTORY REPORTING

The system must have ad hoc reporting capabilities.

Product listings of needed assets should conform to the needs of NMIN-FACS purchasing module.

Reporting capabilities should include support for automatic asset depreciation recording for input into MAIN-FACS or the state's annual financial statement.

The system must have ad hoc reports to assist in planning the installation of new releases and version of software.

4.0 REMOTE TROUBLESHOOTING:
4.1 REMOTE CONTROL OF CLIENTS

Product must have the capability to remotely log-on to remote workstations.

Product must allow a user to be able to prevent remote control of his/her client workstation.

Product must limit remote control by administrators to only their respective domains.

Product must have the capability to reboot a remote workstation.

Product must provide for execution of programs on remote workstations.

Product must be able to display various diagnostic information about the workstation including:
CMOS information
Device Drivers
IRQ Usage
Programs currently loaded in memory
DOS interrupt vectors
Hard Disk usage
Windows class modules loaded in memory
Windows GDI and Global Heaps
CPU
Product must be able to display various hardware configuration information including:
Number of serial ports
Number of parallel ports
Modem information
Amount of RAM
Size of hard disk
BIOS & NICs

Product must be able to display present and previous inventory/configuration information to support problem resolution.

Product must be able to transfer files to remote client workstations.

Help desk staff must be able to remotely modify configuration files to resolve user problems.

Product must have security to prevent inappropriate use of the system (vendors will need to elaborate on provisions here).

Product must include a remote control activity audit trail.

4.2 REMOTE- SERVER MANAGEMENT

Product must support alarms for various events. (i.e. free disk space is less than 5%)

Product must support remote reboot of servers.

Product must support remote execution of programs on the server.

4.3 ALERTS

Product must support alarms which alert the network control center of various problems, including low disk space, security violations, etc.

Alerts must be logged in a database for later review and trend analysis.

A filter capability must exist to screen alerts or warnings which do not meet a certain threshold.

Alarms should be sent in SNMP format, if desired.

All functions or capabilities (e.g., inventory discovery, software distribution, remote control, etc.) listed above must be provided for the following platforms and network features.

5.0 INFRASTRUCTURE REQUIREMENTS:
5.1 TARGET PLATFORM SUPPORT

DOS workstations.
Windows workstations (3.1, 95, NT, and Workgroups).
OS/2 workstations.
Macintosh workstations.
Intergraph workstations.

UNIX workstations including:
IBM AIX
Hewlett-Packard HP/UX
Unisys U6000 (recognize likely need for enhancement)
Sun Solaris
SCO Unix
The ESD should support the Desktop Management Interface standard developed by the Desktop Management Task Force.

The ESD must support the Windows 95 operating system.

Machines with multi-boot configurations

5.2 TARGET NETWORK SUPPORT

Product should be protocol independent, but must operate within the following networks and topologies:
Novell NetWare networks.
Windows NT networks.
Banyan Vines Networks.
TCP/IP networks.
Workstation ESD agent (if any) must be Winsock compliant for TCP/IP networks.
X.25 connections.
Frame (Ameritech CBDS service) relay connections.
ISDN connections.
Unisys/Burroughs multi-drop poll-select for non switched private lines.

5.3 AVAILABLE PLATFORMS FOR DOMAIN DISTRIBUTION SERVERS

The state requires that its EAM architecture not introduce new operating system requirements on its agencies.

The following listing of network servers are the only ones acceptable to the state for the operation of domain distribution servers:
Novell 3.11+
SCO Unix
Sun OS
OS/2
Windows NT
Solaris
Banyan Vines
Unisys U6000
Macintosh v.7
HP-UX

***